This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

This Page Blank (uspto)

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 685 520**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **91 16008**

(51) Int Cl[5] : G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 23.12.91.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 25.06.93 Bulletin 93/25.

(56) **Liste des documents cités dans le rapport de recherche** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *MONETEL (SA)* — FR.

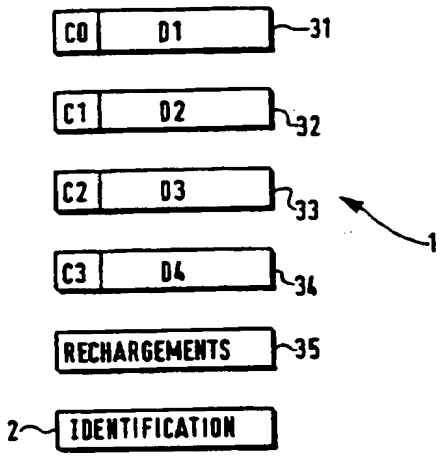
(72) **Inventeur(s)** : Dupuis Serge.

(73) **Titulaire(s)** :

(74) **Mandataire** : Cabinet Bloch Conseils en Propriété Industrielle.

(54) Carte à mémoire rechargeable, procédé de sécurisation et terminal d'utilisation.

(57) L'invention concerne un procédé de sécurisation d'un carte à mémoire passive (40) comprenant au moins une zone (31-34) de mémoire effaçable formant compteur d'unités de crédit et au moins une zone (35) de mémoire non effaçable formant compteur de rechargements, dans lequel on compare à chaque utilisation de la carte un certificat inscrit sur la carte à un certificat calculé à partir de données inscrites sur la carte. A cet effet, il comprend les étapes (54) consistant, au moins lors de certains rechargements de la carte, à recalculer ledit certificat en fonction des données de ladite zone de mémoire non effaçable modifiées lors desdits rechargements, et à inscrire le certificat ainsi calculé dans une partie prédéterminée (C0-C3) de la zone de mémoire effaçable.



FR 2 685 520 - A1

BNSDOCID: <FR__2685520A1_I_>

La présente invention concerne une carte à mémoire passive ainsi qu'un terminal pour son utilisation et un procédé permettant de la sécuriser.

On connaît divers types de cartes à mémoire plus ou moins complexes. Les plus simples fonctionnent en écriture seulement, sans protection. A l'autre extrémité, on trouve les cartes à micro-processeur permettant d'utiliser des algorithmes de sécurisation complexes mais qui présentent l'inconvénient d'être d'un prix de revient relativement élevé.

Entre ces deux types de cartes à mémoire, se trouvent les cartes à logique cablée susceptibles d'être rechargées. Ces cartes présentent l'avantage d'être rechargeable ce qui leur confère une longue durée d'utilisation pour une capacité de mémoire relativement limitée, et par conséquent pour un faible coût.

De façon connu, la mémoire de ces cartes rechargeables est généralement organisée de la manière suivante.

Une première partie de la mémoire est accessible uniquement en lecture et contient des données d'identification comme par exemple le numéro de série de la carte.

L'autre partie de la mémoire est affectée au crédit disponible, par exemple à un certain nombre d'unités de taxation téléphonique. Cette partie comporte elle-même une zone effaçable et une zone non effaçable. L'utilisation du crédit inscrit en zone effaçable correspond à un chargement de la carte. Lorsque ce crédit est épuisé, on peut recourir à un nouveau chargement de la carte, l'inscription de ce rechargement étant porté dans la zone non effaçable, tandis

BNSDOCID: FR 2685520A1 I

que la zone effaçable est effacée. Bien entendu, l'effacement de la zone effaçable ne peut se produire qu'après inscription du rechargement correspondant dans la zone non effaçable.

Lorsque toute la zone non effaçable à été inscrite, il est par conséquent devenu impossible de procéder à un nouveau rechargement de la carte qui est devenue hors d'usage.

Typiquement, la deuxième partie de la carte est organisée sous forme de compteurs en cascade, la logique étant cablée de telle sorte que le contenu d'un compteur ne peut être effacé qu'après une inscription dans le compteur de poids immédiatement supérieur. On comprend dans ces conditions que tous les compteurs à l'exception de celui de poids le plus fort sont effaçables, ce dernier étant pour sa part non effaçable.

Il est également connu dans le but de sécuriser un tel type de carte, de calculer à chacune de ses utilisations, un certificat fonction de ses données d'identification et de le comparer à un certificat inscrit dans la partie de la mémoire accessible en lecture seulement. En cas de discordance entre ces deux certificats, la carte est rejetée. Un tel procédé de sécurisation permet d'éviter l'utilisation du certificat d'une carte pour en recharger une autre.

Un tel procédé présente toutefois l'inconvénient d'utiliser un certificat unique tout au long de la durée de vie de la carte.

La présente invention vise notamment à fournir un nouveau procédé de sécurisation dans lequel le certificat évolue de façon irréversible durant toute la durée de vie de la carte.

A cet effet l'invention à tout d'abord pour objet un procédé de sécurisation d'une carte à mémoire passive comprenant au moins une zone de mémoire effaçable formant compteur d'unités de crédit et au moins une zone de mémoire non effaçable formant compteur de rechargements, dans lequel on compare à chaque utilisation de la carte un certificat inscrit sur la carte à un certificat calculé à partir de données inscrites sur la carte, caractérisé par le fait qu'il comprend les étapes consistant au moins lors de certains rechargements de la carte, à recalculer ledit certificat en fonction des données de ladite zone de mémoire non effaçable modifiées lors desdits rechargements, et à inscrire le certificat ainsi calculé dans une partie prédéterminée de la zone de mémoire effaçable.

Ainsi, au moins lors de certains rechargements de la carte le certificat est modifié. Du fait que le calcul du nouveau certificat prend en compte au moins certaines données contenues dans le compteur de rechargement, ce certificat varie de manière irréversible puisque, comme on l'a vu ci-dessus, le compteur de rechargement n'est pas effaçable et varie de manière irréversible.

La présente invention à également pour objet un terminal d'utilisation de carte à mémoire passive, pour carte comprenant au moins une zone de mémoire effaçable formant compteur d'unités de crédit et au moins une zone de mémoire non effaçable formant compteur de rechargements, ledit terminal comprenant des moyens pour calculer un certificat à partir de données inscrites sur la carte et comparer ce certificat à un certificat inscrit sur la carte, caractérisé par le fait que lesdits moyens sont agencés pour calculer ledit certificat en fonction au moins de données contenues dans la zone de mémoire non effaçable, et pour réinscrire, au moins lors de certaines utilisations,

BNSDOCID <FR 2685520A1 I >

un nouveau certificat ainsi calculé dans une partie prédéterminée de la zone de mémoire effaçable.

La présente invention a également pour objet une carte à mémoire comprenant au moins une zone de mémoire effaçable formant compteur d'unités de crédit et au moins une zone de mémoire non effaçable formant compteur de rechargements caractérisé par le fait qu'une partie de la zone de mémoire effaçable est agencée pour recevoir un certificat fonction des données inscrites dans la zone de mémoire non effaçable.

Dans le cas où la zone de mémoire effaçable est organisée sous la forme d'une pluralité de compteurs en cascade, chaque compteur ne pouvant être effacé qu'après qu'une inscription ait eue lieu sur le compteur de poids immédiatement supérieur, ladite partie recevant le certificat peut-être répartie sur les différents compteurs ou au contraire être formée soit du compteur de poids le plus fort, soit du compteur de poids le plus faible.

On décrira maintenant à titre d'exemple non limitatif, un mode de réalisation particulier de l'invention en référence aux dessins schématiques annexés dans lesquels :

la figure 1 illustre les différents emplacements de mémoire d'une carte selon l'invention,

la figure 2 représente un terminal d'utilisation de cette carte et,

la figure 3 est un organigramme illustrant le procédé selon l'invention.

BNSDOCID: <FR___2685520A1_I_>

La mémoire 1 de la carte selon l'invention comporte tout d'abord une première partie 2 d'identification accessible uniquement en lecture ,comportant par exemple des données propres au circuit intégré utilisé et un numéro de série de la carte.

Le restant de la mémoire est organisée sous la forme de 5 compteurs à 8 bits 31 à 35 disposés en cascade. Les quatres premiers compteurs 31 à 34 sont du type EEPROM donc effaçable, tandis que le dernier compteur 35 est du type PROM donc non effaçable. La logique cablée de la carte est telle qu'un compteur quelconque ne peut être effacé qu'après une écriture sur le compteur de poids immédiatement supérieur. Le compteur 35 ne peut par conséquent pas être effacé.

Les compteurs 31 à 34 sont en outre divisés en une zone débit Di et une zone de certificat Ci. Seules les zones de débit Di sont utilisées pour déterminer le crédit contenu sur la carte.

Lorsque, par exemple, les zones D1 et D2 ont été entièrement écrites, un bit est inscrit dans la zone D3, ce qui permet d'effacer la zone D2 puis, par écriture d'un bit de la zone D2, d'effacer ensuite la zone D1. Lorsque toutes les zones D1 à D4 sont inscrites, il est alors nécessaire de recharger la carte, opération au cours de laquelle un bit est inscrit dans le compteur de rechargement 35 ce qui permet d'effacer successivement D4, D3, D2 puis D1. Par contre lorsque le compteur 35 a été entièrement écrit, il n'est plus possible de le modifier ni, par voie de conséquence, de modifier les compteurs 31 à 34 de sorte que la carte doit être jetée.

Comme montré à la figure 2, la carte 40 comportant la mémoire 1 est placée en utilisation dans un lecteur 41

relié à un micro-processeur 42 programmé de manière à mettre en oeuvre un programme dont l'organigramme est représenté à la figure 3.

La première opération consiste à lire en 50 les données inscrites dans la mémoire 1.

Préalablement à l'utilisation de la carte le micro-processeur calcule et vérifie le certificat en 51.

A cet effet, le micro-processeur calcule :

certificat = f (D1, D2, D3, D4, rechargement, identification)

ou f est une fonction prédéterminée.

Ce certificat est alors comparé au certificat inscrit sur la carte à savoir :

C0, C1, C2, C3

En cas d'égalité de ces deux certificats, la carte peut être utilisée en 52.

On remarquera qu'avec une fonction f telle que précitée, le certificat peut varier à chaque unité consommée puisqu'il dépend de D1. Une autre fonction peut bien entendu être choisie.

C'est ainsi que si le certificat ne dépend pas de D1, il ne changera que toutes les N1 unités consommées, où Ni et le nombre de bits contenues dans la zone Di. De même, si le certificat ne dépend ni de D1, ni de D2, il ne variera que toutes les N1 x N2 unités consommées et ainsi de suite.

BNSDOCID: <FR___2685520A1_I_>

Enfin si le certificat ne dépend que du compteur de rechargement 35, alors il ne sera réactualisé qu'à chaque rechargement de la carte.

Après utilisation de la carte, le micro-processeur détermine en 53 comme cela vient d'être décrit ci-dessus si un nouveau certificat doit être calculé.

Dans ce cas, le micro-processeur calcule en 54 ce nouveau certificat et l'inscrit dans les zones C0 à C3 de la mémoire.

Bien entendu, l'inscription d'un nouveau certificat peut être réalisée par un terminal spécifiquement dédié à la fonction de rechargement.

Le certificat étant dans tous les cas fonction du contenu du compteur de rechargement 35, contenu variant de façon irréversible du fait du caractère non effaçable de ce compteur, le certificat variera lui-même de façon irréversible au cours de la durée de vie de la carte.

On a prévu ci-dessus de répartir les zones C0 à C3 réservées au certificat sur les quatres compteurs 31 à 34.

D'autres possibilités sont bien entendues envisageables.

C'est ainsi que le compteur 31 de poids le plus faible peut être réservé à l'inscription du certificat. Dans ce cas, le certificat est effacé à chaque débit d'une unité et peut être réinscrit avec une valeur différente.

Si par contre, le compteur 34 de poids le plus fort est réservé au certificat, alors il ne peut être modifié qu'au rechargement puisque le compteur 34 n'est effaçable et donc modifiable qu'après une modification du compteur 35.

REVENDICATIONS

1. Procédé de sécurisation d'un carte à mémoire passive (40) comprenant au moins une zone (31-34) de mémoire effaçable formant compteur d'unités de crédit et au moins une zone (35) de mémoire non effaçable formant compteur de rechargements, dans lequel on compare à chaque utilisation de la carte un certificat inscrit sur la carte à un certificat calculé à partir de données inscrites sur la carte, caractérisé par le fait qu'il comprend les étapes (54) consistant, au moins lors de certains rechargements de la carte, à recalculer ledit certificat en fonction des données de ladite zone de mémoire non effaçable modifiées lors desdits rechargements, et à inscrire le certificat ainsi calculé dans une partie prédéterminée (C0-C3) de la zone de mémoire effaçable.

2. Terminal d'utilisation de carte à mémoire passive, pour carte comprenant au moins une zone de mémoire effaçable formant compteur d'unités de crédit et au moins une zone de mémoire non effaçable formant compteur de rechargements, ledit terminal comprenant des moyens (42) pour calculer un certificat à partir de données inscrites sur la carte et comparer ce certificat à un certificat inscrit sur la carte, caractérisé par le fait que lesdits moyens sont agencés pour calculer ledit certificat en fonction au moins de données contenues dans la zone de mémoire non effaçable, et pour réinscrire, au moins lors de certaines utilisations, un nouveau certificat ainsi calculé dans une partie prédéterminée de la zone de mémoire effaçable.

3. Carte à mémoire comprenant au moins une zone de mémoire effaçable formant compteur d'unités de crédit et au moins une zone de mémoire non effaçable formant compteur de rechargements, caractérisée par le fait qu'une partie de la zone de mémoire effaçable est agencée pour recevoir un

BNSDOCID: <FR__2685520A1_I_>

certificat fonction des données inscrites dans la zone de mémoire non effaçable.

4. Carte à mémoire selon la revendication 3, dans laquelle la zone de mémoire effaçable est organisée sous la forme d'une pluralité de compteurs en cascade, chaque compteur ne pouvant être effacé qu'après qu'une inscription ait eu lieu sur le compteur de poids immédiatement supérieur, ladite partie recevant le certificat étant répartie sur les différents compteurs.

5. Carte à mémoire selon la revendication 3, dans laquelle la zone de mémoire effaçable est organisée sous la forme d'une pluralité de compteurs en cascade, chaque compteur ne pouvant être effacé qu'après qu'une inscription ait eu lieu sur le compteur de poids immédiatement supérieur, ladite partie recevant le certificat étant formée du compteur de poids le plus fort.

6. Carte à mémoire selon la revendication 3, dans laquelle la zone de mémoire effaçable est organisée sous la forme d'une pluralité de compteurs en cascade, chaque compteur ne pouvant être effacé qu'après qu'une inscription ait eu lieu sur le compteur de poids immédiatement supérieur, ladite partie recevant le certificat étant formée du compteur de poids le plus faible.

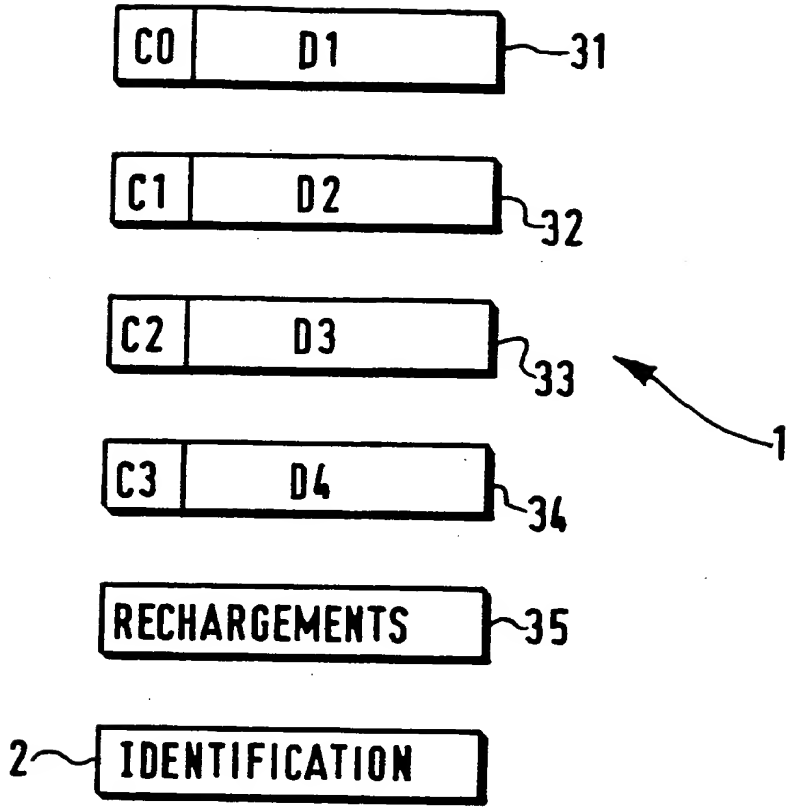


FIG.1

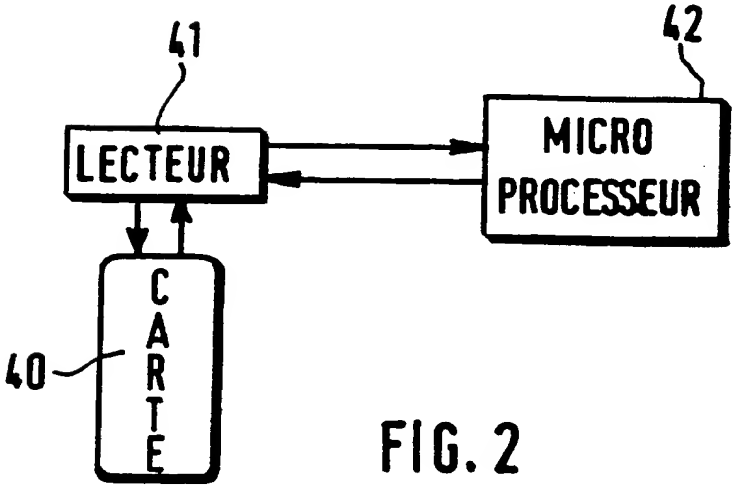


FIG. 2

BNSDOCID: <FR___2685520A1_I_>

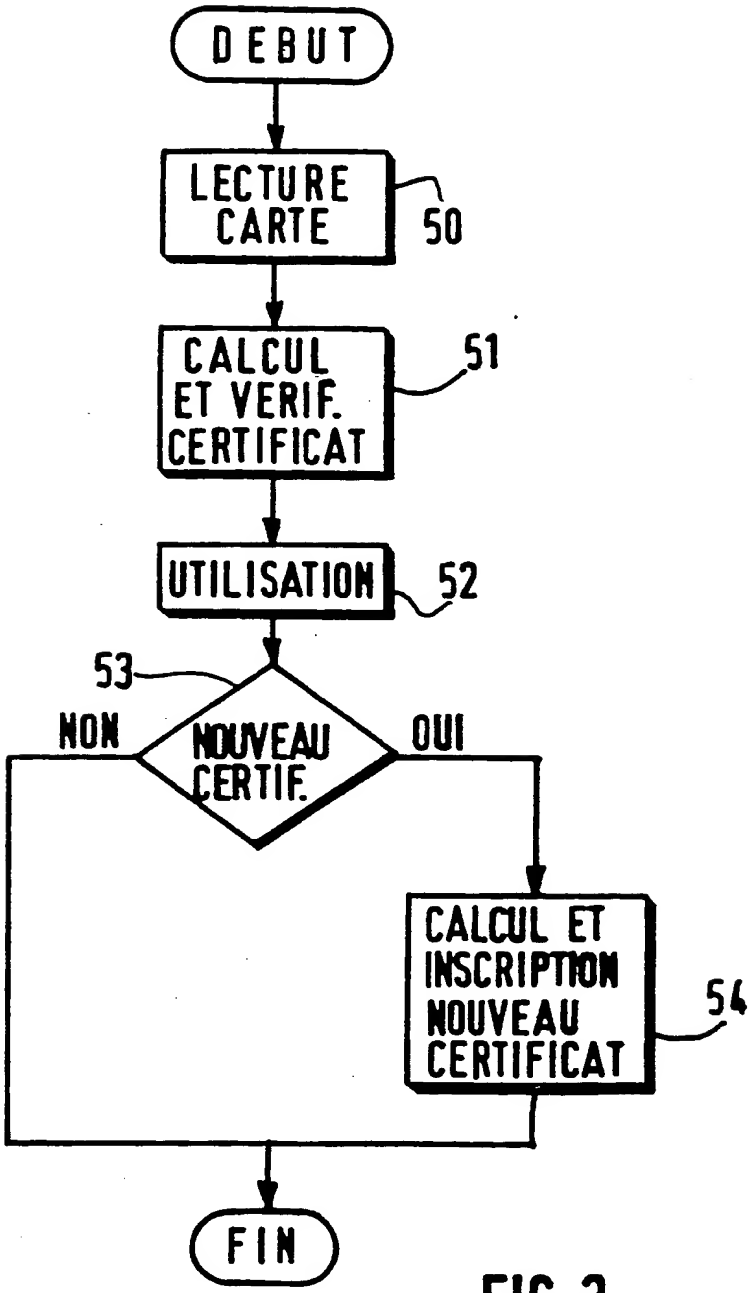


FIG. 3

BNSDOCID <FR 2685520 >

REPUBLIQUE FRANÇAISE

2685520

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national
FR 9116008
FA 465473

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	EP-A-0 423 035 (GEMENOS) * abrégé; figures * * colonne 3, ligne 47 - colonne 6, ligne 14 *	1-3
Y	EP-A-0 378 454 (GEMPLUS CARD INTERNATIONAL) * abrégé; revendications; figure *	1-3
A	DE-A-3 432 557 (ROBERT BOSCH) * le document en entier *	1-3
A	FR-A-2 659 768 (SEXTANT AVIONIQUE) * abrégé; revendications; figures *	1-4

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G07F

2

Date d'achèvement de la recherche
22 SEPTEMBRE 1992

Examinateur
DAVID J.Y.H.

EPO FORM 1503 03.82 (P0413)

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

BNSDOCID: <FR___2685520A1 I >

This Page Blank (uspto)